FEDERAL DEPOSIT INSURANCE CORPORATION

DIRECTIVE SYSTEM

TYPE AND NUMBER	
Circular 1360.14	
CONTACT Ludmilla Dudinow	TELEPHONE NUMBER (703) 516-1430
DATE June 17, 1997	
DATE OF CANCELLATION *(Bulletins Only)*	

TO: All Divisions and Offices

FROM: Donald C. Demitros, Director
Division of Information Resources Management (DIRM)

SUBJECT: Year 2000 Date Format and Processing Compliance

1. Purpose. This circular ensures that users as well as the designers, developers, maintainers, and purchasers of information technology are aware of potential software and hardware failures associated with the arrival of the Year 2000. It also establishes the Corporation's policy on Year 2000 date format and processing compliance and defines associated roles and responsibilities.

2. Scope. The provisions of this circular apply to all FDIC divisions and offices.

3. Definitions. Definitions of terms are provided in Attachment A.

4. Background. The basis of the Year 2000 date processing problem lies in the fact that many computer systems have been programmed to identify a year using only its last two digits. The first two digits were originally eliminated to save memory. Since there is no accommodation for the full four-digit year, this becomes a serious problem when "00" is used to identify the Year 2000. It not only becomes impossible to distinguish 2000 from 1900, but it also becomes difficult to calculate the passage of time between preceding years and the Year 2000. Once software begins mixing dates in both the 19xx and 20xx ranges, mistakes of varying degrees can result. In some cases, software may fail immediately without completing an operation. In others, it may not fail, but produce erroneous output which could remain undetected for a long time. This computer glitch will affect numeric validations, date comparisons, arithmetic operations, and date dependent sorts.

Although the greatest Year 2000 impact may be on mainframe legacy applications, Year 2000 problems are not restricted to mainframe computers or to a specific programming language. Commercial software packages, distributed database systems, local area networks (LANs), wide area networks (WANs), telecommunication systems, personal computers (PCs), data from external sources, and machinery operating in buildings will also be affected. What makes the problem such a challenge is its tremendous size. Dates can be found everywhere in computer hardware and software. Neither industry nor the Federal government has yet fully determined the scope of this situation. However, estimates as high as $30 billion to fix the problem in Federal agencies are projected. While not all of the FDIC's software and hardware are at risk, timely action now could prevent failures and reduce the need for intense corrective action later.

5. Policy. To ensure that vital FDIC systems do not default due to the date change on January 1, 2000, Corporation policy requires that all systems being procured or under development which are placed in production after June 1, 1997 will be Year 2000 compliant. Exceptions will be allowed only with written permission from the Director, DIRM, after sufficient evidence is presented that the system must go into production to maintain a business process, and that delaying its production to correct Year 2000 processing would cause harm to the FDIC's business. Such exceptions will have a written plan for compliance that includes an assessment of the problem, a solution, a schedule, and an estimated cost to resolve the problem. This applies to all categories of software, including commercial-off-the-shelf (COTS) and custom systems built in-house.

Under this policy, "Year 2000 compliant" means information technology that accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the years 1999 and 2000 and leap year calculations (Year 2000 is a leap year). Furthermore, Year 2000 compliant information technology, when used in combination with other information technology, will accurately process date/time data if the other information technology properly exchanges date/time data with it.

For systems already in production and other information technology acquisitions (e.g. hardware and services), paragraph 6., General Guidelines, below, detail the methodology to be used for remediation.

Detailed guidelines and procedures, such as defining compliant databases, procedures for programming/fixing code, testing the re-engineered programs and systems as well as testing new computer hardware for Year 2000 compliance will be published in future circulars.

6. General Guidelines

a. Approach to Solving Year 2000 Problem . A modified systems life cycle, divided into five phases, is being implemented to solve the Year 2000 problem. The five phases overlap and will progress concurrently as follows.

(1) Awareness . Establishing the FDIC's Year 2000 project and project team, identifying the overall Year 2000 approach, defining compliance standards, and assigning responsibility for corrective actions. Awareness includes a strong emphasis on publicizing the corporate Year 2000 approach.

(2) Assessment . Gathering and analyzing information to determine the size and impact of the Year 2000 problem, including a code inventory and analysis to identify Year 2000 costs, issues, and exposures. Assessment also involves deciding to modify, re-engineer, and retire systems/programs. Primary deliverables are the Project Plan and Master Schedule for Renovation and Validation Phases. At a minimum, the Project Plan shows start and production release dates for each system and major steps to be taken in converting and testing the code, and it establishes the necessary infrastructure and resources required to accomplish these tasks.

(3) Renovation . Implementing standardized date routines, installing Year 2000 tools, modifying system codes, re-engineering Year 2000 vulnerable systems/programs, developing bridges for systems that can't be re-engineered, re-creating missing source code, and changing files and databases.

(4) Validation . Testing re-created code and renovated software for Year 2000 compliance and identifying any errors introduced during renovation. This phase especially involves integration and regression testing.

(5) Implementation . Scheduling the implementation of all changed systems as well as vendor provided software and hardware, resolving data exchange issues, deciding how to handle archive files, and developing backup/recovery plans.

b. Information Technology Acquisition . Consistent with government policy, when acquiring information technology that will be required to perform date/time processing involving dates after December 31, 1999, all orders and contracts will:

(1) Require the information technology to be Year 2000 compliant; or

(2) Require that non-compliant information technology be upgraded to be Year 2000 compliant prior to the earlier of (a) the earliest date on which the information technology may be required to perform date/time processing involving dates later than December 31, 1999 or (b) October 1, 1999.

As appropriate, all solicitations, orders, and contracts will describe existing information technology that will be used with the information technology to be acquired and identify whether the existing information technology is Year 2000 compliant. Acquisition selections that are not Year 2000 compliant must be approved by the Director, DIRM, as described in paragraph 5., Policy, above.

c. Software . The Year 2000 issue affects all system software components and every application at some level. Some applications will require only a quick analysis to ensure compliance. Others will require a full-scale conversion effort.

Once non-compliant applications are identified, a detailed analysis must be performed to identify specific programs, files, and other components that require conversion. Corrective actions, where possible, should be taken during normal systems maintenance or upgrade cycles. However, special consideration should be given to embedded systems that are stored and have a

three year or longer life span. In such cases, out-of-cycle maintenance actions may be necessary.

The level of compliance and impact analysis for all system software components (operating systems, databases, utilities, etc.) must be determined. Although software vendors are responsible for compliance, the timing and installation of releases must be considered. In some cases, replacement software may be required for older components that will not be integrated (such as old versions of compilers). These replacements may cause other side effects or require additional conversion efforts.

PC applications may store data in a number of file formats, some of which are proprietary. Examples include text files, desktop and workgroup database files and word processor and spreadsheet documents. Some PC databases can be used in a Year 2000 safe manner, but many existing schemes will use two-digit date fields (e.g., to minimize database sizes). Affected databases must be identified and brought into compliance.

d. Date Compatibility . The potential to introduce and multiply errors during data exchange is great, and timing considerations are important because either the sending or receiving entity will have to convert its files from one format to another unless both are ready to make Year 2000 changes, simultaneously. Where possible, trading partners of corporate data must agree early on to changes to record formats and schedules for corrective action. They should also provide test files to one another.

When FDIC systems interface with other systems, internal or external to the Corporation, in which the use of the two-digit year is projected to extend into or beyond the Year 2000, it will be necessary to modify existing bridge programs, write temporary or new programs, or change the suppliers of the information to maintain data accuracy.

Further, to ensure data compatibility, all software planned or in process will be developed in accordance with the Federal Information Processing Standards (FIPS) PUB 4-1, “Representation for Calendar Date and Ordinal Date for Information Interchange,” Change Notice 1 (see Attachment B).

e. Hardware. All hardware, whether it is connected to other hardware or it stands alone, whether it is in use or in inventory, must be checked for Year 2000 compliance. This includes all computers, switches, routers, bridges, servers, printers, facsimile machines (FAXs), multiplexers, private branch exchanges (PBXs), and voice processing adjuncts as well as other devices that contain their own central processing units (CPUs). CPUs in mainframe computers and their inherent design as well as any peripherals attached to them must also be checked to determine if they can handle Year 2000 requirements. If it is not in compliance, hardware must either be brought into compliance or retired.

Internal hardware components (e.g., ROM, BIOS chips, intelligent hard disk controllers, etc.) may not properly recognize the Year 2000 and, therefore, will not process the year element for the Year 2000 correctly. To determine if problems exist and correct such problems, the following actions are required:

(1) Identify hardware operating systems that produce and rely on date information.

(2) Analyze hardware components and sub-components to determine which impact operating system date information.

(3) Partner with manufacturers to determine whether products are Year 2000 compliant and develop solutions, if they are not.

All embedded systems in machinery operating in FDIC’s facilities (e.g., in heating, fire alarm, security, elevator systems, etc.) must be reviewed for Year 2000 compliance, and solutions must be developed in partnership with manufacturers and vendors.

7. Roles and Responsibilities

a. Divisions and Offices shall:

(1) Work with DIRM staff to assess the status of all software in use in divisions and offices and identify those which will be in use after 1999 and therefore, require detailed assessment and remediation.

(2) Assist in identifying those business processes which are automated in computer systems that are especially at risk for errors in processing caused by possible date processing errors.

(3) Provide personnel resources for development of test plans and to conduct comprehensive testing of their own remediated systems.

(4) Provide representation to a corporate advisory committee which will work with the DIRM Year 2000 Project Office to:

(a) Ensure all Year 2000 issues are addressed;

(b) Participate in prioritization and coordination of remediation and systems testing to ensure adequate integration testing for systems which share data;

(c) Identify changes in system plans which might affect the approach planned for a given application; and,

(d) Provide division/office certification that remediated systems have fully met all test plan expectations.

b. Division of Administration (DOA) shall:

(1) Locate embedded systems in building machinery (e.g., in heating systems, fire alarm systems, security systems, elevator systems, etc.).

(2) Contact vendors/manufacturers to determine whether or not equipment and machinery running in FDIC facilities is Year 2000 compliant.

(3) Through contracting activities of the Acquisition Services Branch:

(a) Ensure that all contract vehicles include language which requires vendors to deliver Year 2000 compliant products;

(b) Require vendors to warrant fault free performance in the process of date and date dependent data (including, but not limited to, calculating, comparing, and sequencing); and,

(c) For products currently in use at FDIC which are under maintenance contracts, require vendors to provide plans to upgrade their products to be Year 2000 compliant in conjunction with maintenance plan renewals.

Appropriate contract language for new contracts and contracts to be modified is provided in the Year 2000 Clauses (see Attachment C).

c. The Director of DIRM , FDIC's Chief Information Officer, is responsible for leading and supporting FDIC's Year 2000 efforts Corporation-wide. DIRM shall:

(1) Ensure that all software and hardware within their purview is Year 2000 compliant.

(2) Provide overall appraisals of the situation and its impact, major concerns and names and numbers of systems in each of the five phases (awareness, assessment, renovation, validation, and implementation) of addressing the Year 2000 problem.

(3) Plan for and make resource shifts necessary to correct the Year 2000 problem.

(4) Determine which databases require special attention to make them Year 2000 compliant and take appropriate corrective actions (e.g. data conversion).

(5) Examine software and hardware to ensure that dates are processed correctly and take appropriate corrective action if it is not.

(6) Develop plans for any remediation actions needed to resolve Year 2000 problems.

(7) Estimate completion dates for each phase of addressing the Year 2000 problem.

(8) Estimate costs (required, expended, allocated) associated with each phase of addressing the Year 2000 problem.

(9) Fix, retire, replace, or out source particular applications.

(10) Determine the level of commitment from outside suppliers of data to be Year 2000 compliant, and if it is determined that the outside data is not in compliance, prepare FDIC systems to accept and correctly process whatever data is received from the outside systems or review/select other options for ensuring uninterrupted service to the Corporation.

(11) Time and coordinate Year 2000 remediation efforts if applicable to interfaces of affected applications.

(12) Install or modify, where needed, bridge programs to allow coexistence between two-digit and four-digit information or change the supplier(s) of information.

(13) Test re-created code and renovated software for Year 2000 compliance.

(14) Develop and test contingency plans for keeping business functions operating in the event of IT failure due to date related problems, if a vendor fails to provide an adequate Year 2000 solution, or a system cannot be remediated in time.

d. Millennium IT Strategies Section,DIRM shall:

(1) Develop and sustain visibility on the Year 2000 problem until it is satisfactorily resolved.

(2) Determine the scope of the Year 2000 problem, develop an overall corporate approach, and develop the Project Management Plan that addresses each phase of the Year 2000 resolution process.

(3) Monitor progress against the Project Management Plan.

(4) Document FDIC's baseline of systems and hardware inventory, including essential information about them to better address Year 2000 efforts.

(5) Serve as overall contact for pilot projects as well as assessment and remediation services.

(6) Provide project management support for Year 2000 activities throughout the Corporation, including cost estimates for corrective actions as well as planning, scheduling, testing, and coordinating the implementation of the required corrective actions.

(7) In cooperation with the Acquisition Services Branch, contact vendors to determine whether or not their products are Year 2000 compliant and team with them to resolve compliance problems.

(8) Perform risk assessments based on Year 2000 information supplied by application owners and software/hardware vendors.

(9) Assist divisions/offices with Year 2000 issues, as requested.

(10) Recommend additional measures that must be taken to successfully address the Year 2000 problem.

8. Point-of-Contact . The primary FDIC point-of-contact for the Year 2000 project is the Chief, Millennium IT Strategies Section, Development Technology Branch, DIRM.

9. Questions . Questions regarding this circular shall be referred to the Chief, Millennium IT Strategies Section, DIRM, at (703)516-1338.

10. Effective Date . The provisions of this circular are effective immediately.

Attachments

DEFINITIONS

a. Application. A program that performs useful work not related to the computer itself. Depending on the work for which it was designed, an application can manipulate text, graphics, numbers, or a combination of these items.

b. Basic Input-Output System (BIOS). Read-only memory (ROM) software which is responsible for basic boot functions in personal computers and managing pertinent data such as the time and date.

c. Bridge Programs. Receive information in one format, modify it, and put it out in another format. For example, a bridge program can receive the year in a two-digit format, add century information through the use of an algorithm, then write the output with a four-digit year. Where a bridge must accommodate data from a number of sources, it can be table driven to accept the input in either format based upon an entry in the table. However, it will output the data in a fixed four-digit year format. FDIC internal bridges may be built to take an eight-digit date from a remediated system and connect it to digits for a "yet to be" remediated system.

d. Central Processing Unit (CPU). The part of a computer that includes circuits that control the interpretation and execution of computer instructions. It is also called a processor or microprocessor.

e. Corporate Data. All data that supports corporate missions and business functions and/or is shared among FDIC organizations, including data that is imported from, or exported to, external organizations. All data from which business decisions are derived is considered to be corporate data. Although corporate data may be automated, such as that stored via computer applications, it can also include automated data such as card files containing historical institution data of CALL reports submitted in paper form.

f. Data Exchange. The passing of data from one program to another, one system to another, and from one agency to another (e.g., FDIC and the National Finance Center).

g. Database. A collection of logically related records or files. A database consolidates many records that may have been previously stored in separate files so that a common pool of data records serves as a central file for several data processing applications.

h. Embedded System. Special purpose computer system designed for a limited function(s), like that of an elevator, ATM machine, or network concentrator. Such systems run with very little human intervention, functioning automatically. They may be connected to central computers which monitor their performance or they may function independently. Embedded systems must usually be extremely reliable. They must also respond to events in real time (i.e. as they happen, without undue delay).

i. Hardware. Major items of equipment or their components used for a particular purpose (e.g. the physical elements of machinery or a computer system as opposed to the programs or information stored in a machine).

j. Inventory. In the context of a Year 2000 program, the process of determining an agency's computer hardware assets and components that comprise its systems portfolio. The software inventory should include all applications, databases, files, and related system components that require inspection to locate date data and related date computations.

k. Legacy. Anything left over from a previous version of hardware or software. For example, the term "legacy" can be applied to applications from earlier versions of MS-DOS or Windows.

l. Network. A connection of two or more computers for the purpose of communicating or sharing information.

m. Peripheral Device. A device connected to a computer's CPU but that is not part of that unit (e.g. a terminal, tape drive, disk drive, printer, mouse, and keyboard).

n. Read-Only Memory (ROM). Permanent memory that is usually housed in a chip or chip set on the computer system board. ROM generally contains information that the computer processor needs to do its job (i.e., information about the computer that does not change even when the power is turned off).

o. Remediation. The act or process of remedying or correcting.

p. Router. A hardware device that controls two or more networks and routes incoming data packets to the appropriate network.

q. Server. A hardware or software product that stores information and controls the dissemination and movement of information.

r. Software. Programs that tell a computer what to do. Software can be classified into system software (e.g. operating system software which gets the computer up

and running) and applications software (e.g. word processing, spreadsheet, and database management software).

s. System. In the context of this circular, "system" may refer to computer hardware (in various forms), computer software (either operating or application), as well as other equipment such as FAX machines, PBXs, elevators, and virtually anywhere a computer chip exists.

t. Year 2000 Problem. The potential problems and its variations that might be encountered in any level of computer hardware and software from microcode to application programs, files, and databases that need to correctly interpret year-date data represented in two digit-year format.

National Institute of Standards and Technology (NIST)
FIPS PUB 4-1 Representation for Calendar Date and Ordinal Date
for Information Interchange
CHANGE 1, March 25, 1996

Specific Change

"For purposes of electronic data interchange in any recorded form among U.S. Government agencies, NIST highly recommends that four-digit year elements be used. The year should encompass a two-digit century that precedes, and is contiguous with, a two-digit year-of-century (e.g., 1999, 2000, etc). In addition, optional two-digit year time elements specified in ANSI X3.30-1985 (R1991) should not be used for the purposes of any data interchange among U.S. Government agencies."

Year 2000 CLAUSES
FEDERAL DEPOSIT INSURANCE CORPORATION

Year 2000 Warranty--Commercial Supply Items

The contractor warrants that each hardware, software, and firmware product delivered under this contract shall be able to accurately process date related data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the year 1999 and the year 2000, including leap year calculations, when used in accordance with the product documentation provided by the contractor, provided that all products (e.g. hardware, software, firmware) used in combination with such delivered product properly exchange date related data with it. If the contract requires that the delivered products must perform as a system in accordance with the foregoing warranty, then that warranty shall apply to those delivered products as a system. The duration of this warranty and the remedies available to the Government for breach of this warranty shall be as defined in, and subject to, the terms and limitations of the contractor's standard commercial warranty except when specific warranties are contained in this contract. Notwithstanding any provision in such commercial warranty or warranties, at time of delivery of purchased item, contractor will perform a demonstration test in the presence of FDIC personnel to confirm that the item complies with this clause. If the item does not comply, it will not be accepted. If the FDIC decides it is not practicable for contractor to perform the demonstration test, contractor will instead, within 5 business days of delivery, provide a certificate to the contracting officer and oversight manager stating that the purchased item complies with this clause. If the certificate is not received, acceptance of the item will be revoked. If non-compliance with the clause is discovered at any time after acceptance but before February 1, 2001, the remedies available to the Government under this warranty shall include repair, replacement or reimbursement for reprocurement of an acceptable replacement product including the full costs of the product itself and all costs associated with its reprocurement. Nothing in this warranty shall be construed to limit any rights or remedies the Government may otherwise have under this contract with respect to defects other than Year 2000 performance.

Year 2000 Warranty--Custom Computer Items

The contractor warrants that each non-commercial item of hardware, software, and firmware delivered or developed under this contract shall be able to accurately process date related data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the year 1999 and the year 2000, including leap year calculations, when used in accordance with the item documentation provided by the contractor, provided that all items (e.g. hardware, software, firmware) used in combination with such delivered or developed item properly exchange date related data with it. If the contract requires that the delivered or developed items must perform as a system in accordance with the foregoing warranty, then that warranty shall apply to those delivered or developed items as a system. The duration of this warranty and the remedies available to the Government for breach of this warranty shall be as defined in, and subject to, the terms and limitations of any general warranty provisions of this contract. Notwithstanding any provision to the contrary in such warranty provision(s), or in the absence of any such warranty provision(s), at time of delivery of purchased item, contractor will perform a demonstration test in the presence of FDIC personnel to confirm that the item complies with this clause. If the item does not comply, it will not be accepted. If the FDIC decides it is not practicable for contractor to perform the demonstration test, contractor will instead, within 5 business days of delivery, provide a certificate to the contracting officer and oversight manager stating that the purchased item complies with this clause. If the certificate is not received, acceptance of the item will be revoked. If non-compliance with the clause is discovered at any time after acceptance but before February 1, 2001, the remedies available to the Government under this warranty shall include repair or replacement. Nothing in this warranty shall be construed to limit any rights or remedies the Government may otherwise have under this contract with respect to defects other than Year 2000 performance.